UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,567	03/28/2001	Soichi Furuya	520.39632VX1	4795

24956 7590 02/22/2007
MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
02/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

Response to Rule 312 Communication	Application No.	Applicant(s)	
	09/818,567	FURUYA ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

1. ☒ The amendment filed on *20 November 2006* under 37 CFR 1.312 has been considered, and has been:

a) ☐ entered.

b) ☐ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☒ entered in part. See explanation below.

The Amednment presented was to correct typrographical errors in claims 9, 21, and 33. After Examiner review the claims still contained typographical errors due to a "<" (less than sign) not being deleted. Examiner contacted attorney of record Carl I. Brundidge on 16 January 2007, who approved the attached Examiner's Amendment to correct typographical errors in the claims.

An examiner's amendment to the record is attached. Please enter entire claim set. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. The examiner's amendment to amend claims 9, 21, and 33; was authorized by attorney of record Carl Brundidge in phone interview on 16 January 2007l.

KAMBIZ ZAND
PRIMARY EXAMINER

EXAMINER'S AMENDMENT:

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims

Claims 1-8 (canceled).

9. (currently amended) A symmetric-key decryption method performed by a computer, comprising the steps of:

dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

performing decryption operations for producing plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

concatenating a series of said ciphertext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the plaintext obtained from the ciphertext has been altered,

wherein one of said decryption operations for producing a plaintext block i corresponding to a ciphertext block i (2 ≤ i[[≤]]-, i being a number indicative of ciphertext blocks) comprises:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said ciphertext block i and said first random number block

corresponding to said ciphertext block i, and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number or said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step.

10. (previously presented)The symmetric-key decryption method as claimed in claim 9, wherein the step of generating random number blocks divides a random number sequence longer than said ciphertext to produce the random number blocks independent of any one of said ciphertext blocks.

11. (original) The symmetric-key decryption method as claimed in claim 10, further comprising steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has been altered.

12. (previously presented)The symmetric-key decryption method as claimed in claim

11, further comprising steps of:

extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key; and

checking said redundancy data and said secret data to detect whether said ciphertext has been altered.

Claims 13-20 (canceled).

21. (currently amended) A symmetric-key decryption apparatus comprising:

a circuit for dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

a random number generation circuit for generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

a decryption operation circuit for performing decryption operations to produce plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

a circuit for concatenating a series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

a circuit for examining the redundancy data to detect whether the plaintext obtained from ciphertext has been altered,

wherein said decryption operation circuit for producing a plaintext block i corresponding to the ciphertext block i (2 ≤i[[≤]]-, i being a number indicative of ciphertext blocks) comprises:

a first circuit for performing a first operation on said ciphertext block i,

a second circuit for performing a second operation on a result of said first operation performed on said ciphertext block i and said first random block corresponding to said ciphertext block i, and

a third circuit for performing a third operation on a result of said second operation performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce a result of said third operation as said plaintext block i, and

wherein said first circuit performs the first operation on said ciphertext block i and a result of said second operation performed on said ciphertext block i-1, and

wherein either said first random number or said second random number, which is generated by said random number generation circuit, is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation.

22. (previously presented)The symmetric-key decryption apparatus as claimed in claim 21, wherein said random number generation circuit divides a random number sequence longer than said series of ciphertext blocks to produce the random number blocks independent of any one of said ciphertext blocks.

23. (previously presented)The symmetric-key decryption apparatus as claimed in claim 22, further comprising:

a circuit for concatenating a plurality of said plaintext blocks to generate plaintext;

a circuit for extracting redundancy data included in said plaintext; and

a circuit for checking said redundancy data to detect whether said ciphertext has been altered.

24. (previously presented)The symmetric-key decryption apparatus as claimed in claim 23, further comprising:

a circuit for extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key,

wherein said circuit for detecting whether said ciphertext has been altered checks said secret data and said redundancy data.

Claims 25-32 (canceled).

33. (currently amended) A medium storing a program for causing a computer to perform a symmetric-key decryption method, wherein said program is read into said computer, said program when executed causes said computer to perform the steps of:

dividing a ciphertext, which is an input text, to generate a plurality of ciphertext blocks each having a predetermined length;

generating a first random number block and a second random number block both corresponding to each of said plurality of ciphertext blocks based on a secret key that is an input value;

performing decryption operations for producing plaintext blocks each corresponding to each of said plurality of ciphertext blocks;

concatenating a series of said plaintext blocks one after another sequentially to output a plaintext, which includes a message and redundancy data; and

examining the redundancy data to detect whether the plaintext obtained from the ciphertext has been altered,

wherein one of said decryption operations for producing a plaintext block i corresponding to a ciphertext block i (2 ≤i[[≤]]-, i being a number indicative of ciphertext blocks) comprises:

a first operation step for performing an arithmetic computation on said ciphertext block i,

a second operation step for performing an arithmetic computation on a result of said first operation step performed on said ciphertext block i and said first random number block corresponding to said ciphertext block i; and

a third operation step for performing an arithmetic computation on a result of said second operation step performed on said ciphertext block i and said second random number block corresponding to said ciphertext block i, to produce said plaintext block i, and

wherein said first operation step performs the arithmetic computation on said ciphertext block i and a result of said second operation step performed on the ciphertext block i-1, and

wherein either said first random number or said second random number is generated in complete isolation from any one of said plurality of ciphertext blocks or the result of said first operation step.

34. (previously presented)The medium storing a program as claimed in claim 33, wherein the step of generating random number blocks divides a random number sequence longer than said ciphertext to produce the random number blocks independent of any one of said

ciphertext block.

35. (original) The medium storing a program as claimed in claim 34, wherein said symmetric-key decryption method further comprises steps of:

concatenating a plurality of said plaintext blocks to generate plaintext;

extracting redundancy data included in said plaintext; and

checking said redundancy data to detect whether said ciphertext has been altered.

36. (previously presented)The medium storing a program as claimed in claim 35, wherein said symmetric-key decryption method further comprises steps of:

extracting secret data included in said plaintext, said secret data, different from either said redundancy data or said message, being data generated based on said secret key; and

checking said redundancy data and said secret data to detect whether said ciphertext has been altered.

Claim 37 (canceled).

38. (previously presented)The symmetric-key decryption apparatus as claimed in claim 22, wherein said random number generation circuit further comprises:

a pseudorandom number generator for generating said random number sequence based on said secret key; and

a circuit for producing said random number blocks from said random number sequence.